

**IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI**

William Johnson, Joshua Kirk, and Toni Reynolds individually and on behalf of all others similarly situated,

Plaintiffs,

v.

Cornerstone National Insurance Company; Accredited Resource Insurance Agency, LLC; James Insurance Agency, Inc.; Reed-Williams Insurance Agency, Inc.; and Guidewire Software, Inc.,

Defendants.

Civil Action No. 22-CV-04135-WJE

**CONSOLIDATED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

Plaintiffs William Johnson, Joshua Kirk, and Toni Reynolds individually, and on behalf of all others similarly situated (“Plaintiffs”), upon personal knowledge of facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Consolidated Class Action Complaint against Cornerstone National Insurance Company (“Cornerstone”); Accredited Resource Insurance Agency, LLC (“Accredited”); James Insurance Agency, Inc. (“James”); Reed-Williams Insurance Agency, Inc. (“Reed-Williams”); and Guidewire Software Inc. (“Guidewire” and collectively “Defendants”), to obtain damages, restitution, and injunctive relief for the Class, as defined below, and allege as follows:

I. INTRODUCTION

1. Every year millions of Americans have their most valuable personal information (“PI”) stolen and sold online because of data breaches and unauthorized data disclosures. Despite warnings about the severe impact of unauthorized data disclosures on Americans of all economic strata, companies—including Defendants—still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data belonging to their customers or potential customers.

2. In the past two years, industry experts have specifically highlighted the importance of driver’s license numbers and the ways in which a coordinated campaign by hackers and malicious attackers is dedicated to collecting those numbers in order to commit identity theft. In fact, a driver’s license is a critical part of a fraudulent, synthetic identity that can be sold on the dark web and is a jackpot for thieves that can be used to create fake driver’s licenses or other fake IDs, open fraudulent accounts, avoid traffic tickets or collect government benefits such as unemployment checks, and use for verification on any government form that requires identity verification. They are also exceptionally useful for fraudsters to craft curated phishing attacks and impersonate government officials to obtain even more information or insert malicious links or attachments into email.

3. Drivers’ license numbers have been taken from auto-insurance providers by hackers in multiple other attacks, including Geico, USAA, Farmers, Kemper, Metromile, and American Family all in 2021, and Elephant Insurance Company in 2022, indicating both that this particular form of PI is in high demand and also that sophisticated insurance agents and companies like Defendants knew or had reason to know that their security

practices were of particular importance to safeguard consumer data. This is especially true given that the New York State Department of Financial Services issued an industry letter on February 16, 2021, stating that the department had recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal the exact kind of information stolen here, and to flag that such information was being used to submit fraudulent claims for pandemic and unemployment benefits.”¹

4. This Action arises out of the recent data breach at Cornerstone, an insurance provider, that targeted consumer information Defendants or Defendants’ subsidiaries, subdivisions, or affiliates had direct access to and/or otherwise had in their possession and/or control.

5. Cornerstone provides automobile and homeowner’s insurance to customers in multiple states throughout the country. Defendants Accredited, James, and Reed-Wiliams are insurance agents connecting to Cornerstone’s databases and information, and selling Cornerstone’s insurance. Defendant Guidewire provides the subscription services connecting the agents with Cornerstone’s databases. Cornerstone “value[s] you as a customer and we understand that your privacy is important.”² And Cornerstone promises

¹ New York Department of Financial Services Industry Letter (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert (last accessed Sept. 11, 2023).

² *Cornerstone National Insurance Company Privacy Policy*, available at: [https://f.hubspotusercontent10.net/hubfs/6858667/CNI_Documents/CNI_Privacy_Policy_\(6-21\)_-Website_and_Portal.pdf](https://f.hubspotusercontent10.net/hubfs/6858667/CNI_Documents/CNI_Privacy_Policy_(6-21)_-Website_and_Portal.pdf) (last visited Sept. 11, 2023).

it does “not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.”³ Cornerstone further promises:

Confidentiality and Security of Personal Information. We restrict access to nonpublic personal information to those employees, agents, representatives or parties who need to know the information in order to provide the products or services requested by our customers. In addition, we maintain physical, electronic and procedural safeguards to protect nonpublic personal information.⁴

6. [REDACTED]

[REDACTED]

7. Defendants failed to meet their promises and obligations to protect the sensitive personal information they collected, maintained, and used. Despite knowing that driver’s license information is highly sensitive and legally restricted as a result of the Driver’s Privacy Protection Act (“DPPA”), 18 U.S.C. § 2724, Defendants failed to secure this highly sensitive information collected from applications, customers, and their online insurance registered agent platform, thereby making it public without consent and in violation of its own corporate promises and policy.

³ *Id.*

⁴ *Id.*

8. [REDACTED]

9. Defendants are legally required to protect the PI they use and gather from unauthorized access and exfiltration. PI is defined as including a person's social security number, driver's license number, name, address, telephone number, and medical or disability information.⁸ Defendants acknowledge this in their privacy policies when they

⁵ Office of the Maine Attorney General, Data Breach Notifications (Aug. 4, 2022), available at: <https://apps.web.maine.gov/online/aeviewer/ME/40/0e2b3fa0-c37d-4645-afca-54ea90420a0e.shtml> (last visited Sept. 11, 2023).

⁶ *Id.*

⁷ *See supra* note 14.

⁸ 18 U.S.C. § 2725(3).

characterize the information they collect, including driver's license numbers, as "nonpublic personal information."⁹

10. As a result of Defendants' failure to provide reasonable and adequate data security, Defendants violated state and federal law by improperly disclosing Plaintiffs' and the Class Members' PI—including their especially sensitive driver's license numbers and the names used to identify them—to unauthorized parties and/or entities. As a direct result of Defendants' acts and/or omissions, the unauthorized parties are already attempting to use the improperly disclosed information to commit identity theft and fraudulently open financial accounts in Plaintiffs' names. Plaintiff Joshua Kirk has already had two incidents of fraud that happened after the breach but before Cornerstone notified him. All Plaintiffs and Class Members are now at much higher risk of continued identity theft and for cybercrimes of all kinds, especially considering the highly valuable and sought-after private PI stolen here, and have suffered damages related to lost time, loss of privacy, and other harms.

11. As such, Plaintiffs bring this Action against Defendants seeking redress for their unlawful conduct, asserting claims for violations of the Driver's Privacy Protection Act, negligence, negligence *per se*, California's Consumer Protection Act, California's Unfair Competition Law, and Declaratory and Injunctive Relief.

⁹ See *supra* note 2; see also Our Privacy Policy (Reed-Williams), available at <https://web.archive.org/web/20210615212343/https://www.reedwilliamsins.com/privacy.html> (last visited Sept. 15, 2023); Privacy Policy (James), available at <https://www.james-insurance.com/privacy-policy> (last visited Sept. 15, 2023).

II. PARTIES

Plaintiff William Johnson

12. Plaintiff William Johnson is a resident of Newport Beach, California. On or about August 4, 2022, Plaintiff Johnson received notice via U.S. mail from Cornerstone that it improperly exposed his PI to unauthorized third parties.

Plaintiff Joshua Kirk

13. Plaintiff Joshua Kirk is a resident of Kingsport, Tennessee. On or about August 4, 2022, Plaintiff Kirk received notice via U.S. mail from Cornerstone that it improperly exposed his PI to unauthorized third parties.

Plaintiff Toni Reynolds

14. Plaintiff Toni Reynolds is a resident of Sacramento, California. In a letter dated August 4, 2022, Plaintiff Reynolds received notice via U.S. mail from Cornerstone that it improperly exposed her PI to unauthorized third parties.

Defendant Cornerstone National Insurance Company

15. Defendant Cornerstone National Insurance Company is a Missouri domestic corporation with a principal place of business at 19 S. Sixth St., Columbia, Missouri, 65201. Cornerstone is licensed to do business and markets, sells, and underwrites automobile insurance policies in Arkansas, Illinois, Indiana, Kansas, Missouri, Oklahoma, and Tennessee, and its websites are accessible throughout the nation.¹⁰

¹⁰ Cornerstone National Insurance Company, <https://www.cornerstonenational.com/>, (last visited Sept. 11, 2023).

Defendant Accredited Resource Insurance Agency, LLC

16. Defendant Accredited Resource Insurance Agency, LLC is an Alabama domestic limited liability company with a principal place of business at 1021 Noble Street, Suite 202, Anniston, AL 36201.

Defendant James Insurance Agency, Inc.

17. Defendant James Insurance Agency, Inc. is an Arkansas domestic corporation with a principal place of business at 114 E Conway Benton, AR 72015.

Defendant Reed-Williams Insurance Agency, Inc.

18. Defendant Reed-Williams Insurance Agency, Inc. is an Oklahoma domestic corporation with a principal place of business at 101 Smith Ave., Ste 3, Poteau, Oklahoma 74953.

Defendant Guidewire Software Inc.

19. Defendant Guidewire Software Inc. is a Delaware domestic corporation with a principal place of business at 2850 S. Delaware St., S-400, San Mateo, California 94403.

20. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

III. JURISDICTION AND VENUE

21. Subject matter jurisdiction in this civil action is authorized pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendants, and the amount in controversy exceeds \$5 million, exclusive of interest and costs.

22. Alternatively, the Court has federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers’ Privacy Protection Act claims and supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

23. This Court has personal jurisdiction over Defendant Cornerstone because it maintains its principal place of business in this District, is authorized to and regularly conducts business in this District and in Missouri, and has sufficient minimum contacts with the State of Missouri. Cornerstone makes decisions regarding the corporate governance and management of its insurance business, including decisions regarding the security measures to protect its customers’ PI, in this District. Cornerstone also intentionally avails itself of this jurisdiction by promoting, selling, and marketing services from Missouri to millions of consumers nationwide.

24. This Court has specific personal jurisdiction over Defendants Accredited, James, and Reed-Williams because their contacts with the State of Missouri are systematic and continuous, and their specific, continuous and systematic contacts give rise to Plaintiffs’ causes of action. *See Dever v. Hentzen Coatings, Inc.*, 380 F.3d 1070, 1073 (8th

Cir. 2004) (Specific jurisdiction is viable where “the injury giving rise to the lawsuit occurred within or had some connection to the forum state.”); *Est. of Logan by & Through Logan v. Busch*, 574 F. Supp. 3d 660, 671 (W.D. Mo. 2021) (“Specific jurisdiction, unlike general jurisdiction, requires a relationship between the forum [state], the cause of action, and the defendant.” (citations omitted)). Here, Accredited, James, and Reed-Williams, individually act as Cornerstone’s agents for the purpose of selling insurance and regularly access Cornerstone’s computer system located in Missouri containing customers’ PI—the activity giving rise to this action. Also, on information and belief, Accredited’s, James’s, and Reed-Williams’s access to Cornerstone’s computer system is based on a contractual agreement with Cornerstone. Customer PI on Cornerstone’s computer system and accessed by Accredited, James, and Reed-Williams allows them to expeditiously quote and sell insurance policies—their core function. Plaintiffs’ claims arise from Accredited, James, and Reed-Williams failing to provide reasonable and adequate security relating to their continuing access to Cornerstone’s computer system in Missouri, thereby facilitating the improper disclosure of Plaintiffs’ and Class Members’ PI to unauthorized parties and/or entities. Therefore, this Court has specific jurisdiction over Defendants Accredited, James, and Reed-Williams because their specific activities in the forum give rise to Plaintiffs’ claims. *Mallory v. Norfolk S. Ry. Co.*, 143 S. Ct. 2028, 2038, 216 L. Ed. 2d 815 (2023) (Specific jurisdiction permits suits arising out of or relating to “a corporate defendant’s activities in the forum State.”); *Gridiron Mgmt. Grp. LLC v. Wranglers*, No. 8:12CV3128, 2012 WL 5187839, at *4 (D. Neb. Oct. 18, 2012) (Special personal jurisdiction found where out-of-state defendant hacked into the computer database of companies in Nebraska

more than 100 times and disseminated private information he obtained; and defendant “should have anticipated the brunt of the injury resulting from his actions would be felt in Nebraska.”).

25. [REDACTED]

[REDACTED]

26. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) through (d) because Defendant Cornerstone resides in this District and, on information and belief, a substantial part of the events or omissions giving rise to Plaintiffs’ and Class Members’ claims emanated from this District, including, without limitation, decisions made by Defendant Cornerstone’s governance and management personnel or inaction by those

individuals that led to misrepresentations, invasions of privacy, and the Unauthorized Data Disclosure.

IV. FACTUAL ALLEGATIONS

A. Defendants' Businesses

27. Cornerstone was founded in 1997. Cornerstone describes itself as an “Insurance Support System.”¹¹ Cornerstone “strive[s] to be your insurance support system for life.” In doing so, Cornerstone “promise[s] to empower you along your unique insurance journey by arming your home and auto policy with the tools it needs to keep what matters most safe at every turn. When you have the right insurance team in your corner, you can stop stressing about the unexpected and start living a little more.”¹² Cornerstone sells automobile and homeowners insurance policies through independent agents in Oklahoma, Illinois, Tennessee, Arkansas, Kansas, and Missouri, “a vast network of experienced independent agents who live and work in your community. They value your time and leave no questions unanswered. Their goal is to pave a clearer path to your insurance satisfaction by offering the one luxury you deserve: options.”¹³

28. Like other insurance providers, Defendants collect various kinds of PI through multiple processes: applications through an online platform used by insurance agents, other application processes and forms, consumer report information, transaction information, and website information.¹⁴ Defendants specifically acknowledge and

¹¹ Cornerstone National Insurance Company, *About*, <https://www.cornerstonenational.com/about> (last visited Sept. 11, 2023).

¹² *Id.*

¹³ <https://www.cornerstonenational.com/> (last visited Sept. 11, 2023).

¹⁴ *See supra* note 2.

designate this information as “nonpublic personal information.” The “nonpublic personal information” collected and stored by Defendants is substantially wider in scope than what Cornerstone reports was accessed and exfiltrated from its network and includes:

- a. Name;
- b. Phone number;
- c. E-Mail address;
- d. Driver’s license number;
- e. Social Security number;
- f. Date of birth;
- g. Marital status;
- h. Vehicle information;
- i. “[I]nformation about other drivers”;
- j. Consumer report information (“information ... obtain[ed] from third party consumer reporting agencies”);
- k. Transaction information (insurance policy information, claims history, billing and payment information);
- l. “information from your transactions with us, our affiliates, or nonaffiliated third parties;” and
- m. Website information (information obtained in part from cookies, such as “Internet Protocol (IP) address, operating system, and session ID”).¹⁵

¹⁵ Cornerstone Privacy Policy, *supra* at n.2.

29. All of this information is extremely valuable.

30. In the course of collecting PI from consumers, including personal information from motor vehicle records Defendants obtain directly from departments of motor vehicles, Defendants promised to provide confidentiality and adequate security for customer data through their applicable privacy policies and through other disclosures.

31. By obtaining, collecting, using and deriving benefits from Plaintiffs' and Class Members' PI, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting this PI from unauthorized disclosure.

32. Plaintiffs and Class Members reasonably relied (directly or indirectly) on these sophisticated companies to keep their sensitive PI confidential, to maintain their systems' security, to use this information for business purposes only, and to make only authorized disclosures of their PI.

33. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PI from involuntary disclosure to third parties.

B. The Unauthorized Data Disclosure

34. In November 2021, Cornerstone “became aware that an unauthorized third party gained access to certain agent user accounts and leveraged this access to run unauthorized searches in these subscription databases.”¹⁶ Following that, “Cornerstone immediately issued a global password reset and notified its software vendor, who conducted a forensic investigation to confirm security. Once the environment was secure,

¹⁶ Notice of Data Breach, filed with the Montana Attorney General, <https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-479.pdf> (last visited Sept. 11, 2023).

we moved forward with a comprehensive analysis into the extent of unauthorized activity.”¹⁷ After an investigation which concluded July 6, 2022, Cornerstone determined that information including names and driver’s license numbers may have been “accessed by an unauthorized third party.”¹⁸ This incident is referred to herein as the “Unauthorized Data Disclosure.”

35. Plaintiffs, along with members of the Class, received a letter from Cornerstone titled, “Notice of Data Security Incident,” dated August 4, 2022. The letter stated that their PI, detailed below, may have been compromised, and included the following:

What Happened and What Information was Involved:

Cornerstone National Insurance Company (“Cornerstone”) is an insurance company located in Missouri. Through its policy management software, Cornerstone and its external agents access various subscription services, including computerized databases where driver’s license information is available for the purpose of performing insurance application due diligence.

On November 29, 2021, Cornerstone became aware that an unauthorized third party gained access to certain agent user accounts and leveraged this access to run unauthorized searches in these subscription databases. Cornerstone immediately issued a global password reset and notified its software vendor, who conducted a forensic investigation to confirm security. Once the environment was secure, we moved forward with a comprehensive analysis into the extent of unauthorized activity.

These investigations, which concluded on July 6, 2022, determined that the following personal information could have been accessed by an unauthorized third party: first name, last name, and driver’s license number.

¹⁷ *Id.*

¹⁸ *Id.*

We have not received information of a specific misuse of any personal information.

What We Are Doing:

Data security is a priority to Cornerstone. Upon detecting this incident we moved quickly to initiate a response, which included the above-referenced communications and investigation, as well as confirming the security of our network environment. We are also reviewing and enhancing our technical safeguards.

Additionally, we are offering you free credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. IDX services include: <<12/24 months>> of credit monitoring and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to <https://response.idx.us/cornerstone> and follow the instructions provided. When prompted please provide the following enrollment code to receive services: <<Enrollment Code>>. IDX is available Monday through Friday, 9:00 am – 9:00 pm EST. Please note the deadline to enroll is **November 4, 2022**.

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call IDX at (833) 423-2977, Monday through Friday, 9:00 am – 9:00 pm EST.

We value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

Cornerstone National Insurance Company¹⁹

36. The Notice confirms Plaintiffs were victims of the Unauthorized Data Disclosure because Defendants collected their information “through [their use of] policy management software,” where “Cornerstone and its external agents access various subscription services, including computerized databases where driver’s license information is available.” The Notice also confirms that driver’s license numbers were acquired when an unauthorized third party “gained access to certain agent user accounts and leveraged this access to run unauthorized searches,” meaning that those numbers were viewed and then accessed by third parties on Cornerstone’s servers.

37. After receiving Unauthorized Data Disclosure notice letters, it is reasonable for Plaintiffs and Class Members in this case to believe that the risk of future harm (including identity theft) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. In fact, Cornerstone’s letter specifically instructs Plaintiffs and the Class: “You should always remain vigilant and monitor your accounts for suspicious or unusual activity.”²⁰ Cornerstone also acknowledges that the Unauthorized Data Disclosure is a source of “frustration, concern, and inconvenience” for Plaintiffs and Class Members. This is because the driver’s license numbers are taken for the purpose of committing fraud in the name of the person whose license information is taken. And because driver’s licenses contain, or can be used to gain access to, uniquely qualifying and

¹⁹ *Id.*

²⁰ *Id.*

comprehensive identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly recommend that immediate notice, replacement, and identity theft protections are put in place for a minimum of 3 years.

38. As a result of the Unauthorized Data Disclosure, approximately 295,867 people had their PI exposed and potentially used for identity theft and fraud by cybercriminals for almost nine months before they were notified of the exposure.

C. The PI Disclosed by Defendants as a Result of Their Disregard for Data Security is Highly Valuable on the Black Market

39. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.²¹ Data breaches, especially those perpetrated against the insurance sector of the economy, have become increasingly widespread.

40. The information Defendants failed to protect in violation of state and federal law is very valuable to phishers, hackers, identity thieves, and cyber criminals, especially at this time where unprecedented numbers of criminals are filing fraudulent unemployment benefit claims and driver's license information is uniquely connected to financial fraud, as well as to the ability to file a fraudulent unemployment benefits claim.

41. Indeed, these hackers often aggregate information taken from data breaches to build profiles on individuals. These profiles combine publicly available information with

²¹ 2019 End of Year Data Breach Report, Identity Theft Center (2019), https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Sept. 11, 2023).

information discovered in previous data breaches and exploited vulnerabilities. There are few data breaches that provide a comprehensive snapshot of any one individual person. Unique and persistent identifiers such as Social Security numbers, driver's license numbers, usernames, and financial account numbers (e.g., credit cards, insurance policy numbers, etc.) are critical to easily forging an identity. When not all information is available, the information that is stolen is used to socially engineer a victim into providing additional information so a "fullz"²² profile can be obtained.

42. For example, a health care system and a retail store point-of-sale system may have two unrelated data breaches where an individual's information is taken. The individual's driver's license number may not be in either of those databases, but after the Unauthorized Data Disclosure, a threat actor could have improved the profile and added a driver's license number. The value of that profile would allow such crimes as identity theft, financial crimes, and even illegal voting that would not previously have been possible.

43. There is no legitimate or legal reason for anyone to use Defendants' inadequate website security to acquire driver's license information of Plaintiffs and the Class. The only reason is for immediate or eventual malicious intent, since no one would go to the trouble of obtaining data that had no value. Any non-public data, especially government issued identification numbers like a driver's license or non-driver's identification number, has criminal value. On the darknet markets, a state issued driver's license number, combined with the full name, is a sought-after data point. Darknet markets

²² "Fullz" is slang used by threat actors and various criminals meaning "full information," a complete identity profile or set of information on any entity or individual.

are a downstream “flea market” for data to be sold, usually not by the original threat actor or criminal group. It is a dumping ground, usually after the data has been exploited.

44. The value of stolen driver’s license information currently has a darknet market (DNM) value of \$1 per license. This was re-verified by experts on March 3, 2022, accessing several DNMs using a trusted identity. Social Security numbers, once considered the “gold standard” of identity fraud, are also selling for \$1 per value in those same markets. This illustrates the value of driver’s license information to cybercriminals and people committing identity fraud. According to popular darknet markets, cyber criminals value driver’s licenses equally to Social Security numbers.

45. In some ways, driver’s license numbers are even more attractive than Social Security numbers to threat actors and more dangerous to the consumer when compromised. Unlike a Social Security number, a driver’s license number is not monitored as closely, so it can potentially be used in ways that will not immediately alert the victim. Threat actors know this as well. Because driver’s licenses contain, or can be used to gain access to, uniquely qualifying and comprehensive identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly recommend that immediate notice, replacement, and identity theft protections are put in place for a minimum of 3 years. Most cyber experts, including Enterprise Knowledge Partners, recommend five years or more.

46. Stolen driver’s licenses can be used (alone or in combination with other information) by malicious actors to accomplish the following:

- Apply for credit cards

- Apply for financial loans (especially student loans)
- Open bank accounts
- Rent a car in the victim's name
- Obtain or create fake driver's licenses
- Given to police for tickets
- Provided to accident victims
- Collect government unemployment benefits
- Create and sell underage fake IDs
- Replace/access account information on:
 - LinkedIn
 - Facebook/Meta
 - WhatsApp
 - Instagram
- Obtain a mobile phone
- Dispute or prove a SIM swap
- Redirect U.S. mail
- Apply for unemployment benefits
- Undocumented individuals may use them as a method to gain access to the U.S., and claim a lost or stolen passport
- Create a fake license as a baseline to obtain a Commercial Driver's License
- File tax returns or gain access to filed tax returns

- Engage in phishing and other social engineering scams

47. Unsecured sites that contain or transmit PI, such as a driver's license numbers, require notice to consumers when the data is stolen because it can be used to perform identity theft and other types of fraud. A threat actor is usually motivated by financial or political gain before it exerts the necessary time and skill to compromise and exfiltrate the PI. Over time, identity thieves have systematized their criminal activities to gather important pieces of a synthetic identity from multiple breaches and sources. The theft of a driver's license number is no less valuable in that endeavor than the theft of a Social Security number, as demonstrated by these two unique identifiers carrying the same price on the darknet, and by the fact that the identity thieves have demonstrated a systematic and businesslike process for collecting these stolen driver's license numbers in this Unauthorized Data Disclosure and others committed against insurers.

48. The frequency of cyberattacks has increased significantly in recent years.²³ In fact, "Cyberattacks rank as the fastest growing crime in the US, causing catastrophic business disruption. Globally, cybercrime damages are expected to reach US \$6 trillion by 2021."²⁴

²³ See *The Cost of Cybercrime*, Accenture Security, available at: <https://web.archive.org/web/20221020185856/https://www.accenture.com/acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf> (last visited Sept. 11, 2023).

²⁴ *Top Cyberattacks of 2020 and How to Build Cyberresiliency*, ISAC, available at: <https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency> (last visited Sept. 11, 2023) (citing Cybersecurity Ventures, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016> (last visited Sept. 11, 2023)).

49. Cybersecurity Ventures, a leading researcher on cybersecurity issues,

expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching \$10.5 trillion USD annually by 2025, up from \$3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.²⁵

50. As noted in recent reports by Deloitte and Interpol, cyberattacks have greatly increased in the wake of the COVID-19 pandemic.²⁶

51. As alleged above, stolen PI is often trafficked on the “dark web,” a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

52. When malicious actors infiltrate companies and exfiltrate the PI that those companies store or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.²⁷ “Why else would

²⁵ Steve Morgan, *Cybercrime To Cost The World \$10.5 Trillion Annually By 2020*, Cybercrime Magazine, Nov. 13, 2020, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016> (last visited Sept. 11, 2023).

²⁶ Deloitte, *Impact of COVID-19 on Cybersecurity*, <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html> (last visited Sept. 11, 2023); Interpol, *Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception*, <https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats> (last visited Sept. 11, 2023).

²⁷ *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, available at: <https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring> (last visited Sept. 12, 2023).

hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

53. Consumers' PI remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²⁸ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.²⁹ Alternatively, criminals are able to purchase access to entire company data breaches for \$900 to \$4,500.³⁰ (Note: the prices can vary depending on the point in the chain – verified identities may sell for higher prices early in the chain, then for the lower prices described above when they reach the “flea market sites.”)

54. The information compromised in the Unauthorized Data Disclosure is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card

²⁸ Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Sept. 12, 2023).

²⁹ Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Sept. 12, 2023).

³⁰ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Sept. 12, 2023).

accounts. And the information compromised in the Unauthorized Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards, as well as benefits accounts in various state benefits offices, compounding the identity theft and cycle of black market sales detailed above. The driver's license numbers compromised in this Unauthorized Data Disclosure are also more valuable because driver's license numbers are long lasting, and difficult and problematic to change.

55. Recently, Forbes writer Lee Mathews reported on Geico's unauthorized data disclosure that included driver's license numbers:

Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200.³¹

56. National credit reporting company, Experian, blogger Gayle Sato also emphasized the value of driver's license information to thieves and cautioned:

Your driver's license may not seem like a jackpot for thieves, but it can be used to create fake driver's licenses, open accounts in your name, avoid traffic tickets or collect government benefits such as unemployment checks. Worse, if your license data has been stolen in a data breach, you may not even know it's being misused.³²

³¹ Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, (April 20, 2021), available at: <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658> (last visited Sept. 12, 2023).

³² Gayle Sato, *What Should I Do If My Driver's License Number Is Stolen?* (Nov. 3, 2021), available at: <https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/> (last visited Sept. 12, 2023).

57. In fact, according to CPO Magazine, which specializes in news, insights and resources for data protection, privacy and cyber security professionals,

To those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: ". . . It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email."³³

58. Driver's license numbers have been taken from auto-insurance providers by hackers in other circumstances, including Geico, Farmers, USAA, Elephant and American Family, all in the last two years, indicating both that this particular form of PI is in high demand³⁴ and also that Defendants knew or had reason to know that their security practices were of particular importance to safeguard consumer data.³⁵

³³ Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, (April 23, 2021), available at: <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/> (last visited Sept. 12, 2023).

³⁴ *Id.*

³⁵ See United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), available at:

59. In fact, when Geico announced that its online quoting platform was subject to a breach, its data breach notice filed with the California Attorney General explicitly stated that GEICO had “reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name.”³⁶

60. Further, an article on TechCrunch explains that it is driver’s license or non-driver’s identification numbers themselves that are the critical missing link for a fraudulent unemployment benefits application: “Many financially driven criminals target government agencies using stolen identities or data. But many U.S. states require a government ID — like a driver’s license — to file for unemployment benefits. To get a driver’s license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer’s driver’s license number. That allows the fraudsters to obtain unemployment benefits in another person’s name.”³⁷

https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuaquis2.htm?m=1819035-01022021 (last visited Sept. 12, 2023) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers’ license number Data Disclosure on January 19, 2021); Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021), available at: <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last visited Sept. 12, 2023) (describing a scam involving drivers’ license numbers and Progressive Insurance).

³⁶ See <https://www.documentcloud.org/documents/20618953-geico-data-breach-notice> (GEICO notice filed with California Attorney General dated April 9, 2021) (last visited Sept. 12, 2023).

³⁷ Zach Whittaker, *Geico Admits Fraudsters Stole Customers’ Driver’s License Numbers for Months*, TechCrunch (Apr. 19, 2021), <https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,benefits%20in%20another%20person's%20name> (last visited Sept. 12, 2023).

61. In addition, the New York State Department of Financial Services issued an industry letter on February 16, 2021, stating that they had “recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal [nonpublic information, including] websites that provide an instant quote. . . . [I]t received reports from two auto insurers in late December 2020 and early January 2021, that cybercriminals were targeting their websites that offer instant [] quotes [] to steal unredacted driver’s license numbers. . . . DFS has confirmed that, at least in some cases, this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits . . . DFS [] has also discovered communications on cybercrime forums offering to sell techniques to access driver’s license numbers from auto insurance websites and step-by-step instructions on how to steal them.”³⁸

62. Once PI is sold, it is often used to gain access to various areas of the victim’s digital life, including bank accounts, social media, credit card, and tax details, or to fraudulently manufacture new accounts for access and sale. This can lead to additional PI being harvested from the victim, as well as PI from family, friends and colleagues of the original victim.

63. Victims of driver’s license number theft also often suffer unemployment benefit fraud, harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts. Unauthorized data disclosures facilitate identity theft as hackers obtain consumers’ PI and thereafter use it to

³⁸ See *supra* note 1.

siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PI to others who do the same.

64. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PI to open financial accounts, receive government benefits, make purchases and secure credit in a victim's name.³⁹ The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."⁴⁰

D. Defendants Were on Notice of the Sensitive and Private Nature of the PI They Stored, Accessed, and Utilized for Insurance Quotes, and Their Duty to Safeguard the PI

65. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PI and of the foreseeable consequences if their data security systems were breached, including the significant costs that would be imposed on Plaintiffs and the Class as a result of a breach.

66. Defendants knowingly refrained from implementing basic security measures to protect Plaintiffs' and Class Members' PI, including information obtained from motor

³⁹ See Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), available at: <http://www.gao.gov/assets/270/262899.pdf> (last visited Sept. 12, 2023).

⁴⁰ *Id.*

vehicle records, in spite of having control over the configuration and design of Cornerstone's quoting platform.

67. In fact, NYSDFS, in its February 16, 2021, industry letter, recommended the following steps for entities that maintain public-facing websites:

- a. Conduct a thorough review of website security controls, including but not limited to a review of its Secure Sockets Layer (SSL), Transport Layer Security (TLS), and HTTP Strict Transport Security (HSTS and Hypertext Markup Language (HTML) configurations.
- b. Review websites for browser web developer tool functionality. Verify and, if possible, limit the access that users may have to adjust, deface, or manipulate website content using web developer tools on the public-facing websites.
- c. Review and confirm that its redaction and data obfuscation solution for NPI is implemented properly throughout the entire transmission of the NPI until it reaches any website.
- d. Ensure that privacy protections are up to date and effectively protect NPI by reviewing who is authorized to see NPI, which applications use NPI, and where NPI resides.
- e. Search and scrub public code repositories for proprietary code.
- f. Block the IP addresses of the suspected unauthorized users and consider a quote limit per user session.⁴¹

68. NYSDFS also recommended that "[t]o combat this cybercrime, the following basic security steps should be implemented...

⁴¹ Industry Letter, *supra*, note 1. Note that this Industry Letter was reported online on numerous websites, including: <https://digitalguardian.com/blog/public-facing-financial-services-sites-ripe-data-theft> (Feb. 23, 2021); <https://www.gravoc.com/2021/04/09/cyber-fraud-alert-issued-for-websites-collecting-npi/> (Apr. 9, 2021); and https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert (Feb. 16, 2021).

- a. **Disable prefill of redacted NPI.** Avoid displaying prefilled NPI, especially on public-facing websites.
- b. **Install Web Application Firewall (WAF).** WAFs help protect websites from malicious attacks and exploitation of vulnerabilities by inspecting incoming traffic for suspicious activity.
- c. **Implement CAPTCHA.** Cybercriminals use automated programs or “bots” to steal data. Completely Automated Public Turing Tests (“CAPTCHA”) attempt to detect and block bots.
- d. **Improve Access Controls for Agent Portals.** Agent portals typically allow agents access to consumer NPI, and robust access controls are required by DFS’s cybersecurity regulation. Measures that should be implemented include:
 - MFA;
 - Robust password policy; and
 - Limitations on login attempts.
- e. **Training and awareness.** Employees and agents should be trained to identify social engineering attacks. Employees and agents should know not to disclose NPI, including DLNs, over the phone. Robotic scripts with grammatical errors or repeated statements used during dialogue are key identifiers of fraudulent calls.
- f. **Limit access to NPI.** Employees and agents should only have access to sensitive information that is necessary to do their job.
- g. **Wait until payments have cleared before issuing a policy.** Auto insurers should consider waiting until an eCheck, credit card, or debit card payment has been cleared by the issuing bank before generating an online policy and granting the policyholder access to NPI.
- h. **Protect NPI received from data vendors.** Ensure that APIs used to pull data files, including JSON and XML, from data vendors are not directly accessible for the internet or agent portals.⁴²

⁴² Industry Letter, New York Department of Financial Services Industry Letter (March 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup, (last visited Sept. 8, 2023) (emphasis in original) (citations omitted).

69. “Insurance companies are desirable targets for cyber attackers because they work with sensitive data.”⁴³ In fact, according to the Verizon 2020 Data Breach Investigations Report, there were 448 confirmed data breaches in the financial and insurance industries.⁴⁴

70. In 2021, drivers’ license numbers were taken from auto-insurance providers by hackers in multiple attacks on similar companies, including Geico, Farmers, USAA, Kemper, Metromile, and American Family. This proves this particular form of personal information is in high demand by hackers and also that sophisticated insurance companies like Defendants knew or were on notice that their security practices were of particular importance to safeguard consumer data.

71. Cornerstone claims, “[W]e value the security of the personal data that we maintain.”⁴⁵ Cornerstone “value[s] you as a customer and we understand that your privacy is important.”⁴⁶ And Cornerstone promises it does “not disclose any nonpublic personal

⁴³ Data Protection Compliance for the Insurance Industry (October 7, 2020), *available at*: <https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry> (last visited Feb. 15, 2022).

⁴⁴ 2020 Data Breach Investigations Report, Verizon, *available at*: <https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf> (last visited Feb. 15, 2022).

⁴⁵ *See supra* note 14; *see also* Our Privacy Policy (Reed-Williams), *available at* <https://web.archive.org/web/20210615212343/https://www.reedwilliamsins.com/privacy.html> (last visited Sept. 15, 2023).

⁴⁶ *See supra* note 2; *see also* Our Privacy Policy (Reed-Williams), *available at* <https://web.archive.org/web/20210615212343/https://www.reedwilliamsins.com/privacy.html> (last visited Sept. 15, 2023).

information about our customers or former customers to anyone, except as permitted by law.”⁴⁷ Cornerstone further promises:

Confidentiality and Security of Personal Information. We restrict access to nonpublic personal information to those employees, agents, representatives or parties who need to know the information in order to provide the products or services requested by our customers. In addition, we maintain physical, electronic and procedural safeguards to protect nonpublic personal information.⁴⁸

72. [REDACTED]

[REDACTED]

73. [REDACTED]

[REDACTED]

⁴⁷ *Id.*

⁴⁸ *See supra* note 2.

74. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

E. Defendants Failed to Comply with Federal Trade Commission Requirements

75. Federal and state governments established security standards and issued recommendations to minimize unauthorized data disclosures, and the resulting harm to individuals and financial institutions. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁴⁹

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.⁵⁰ Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement

⁴⁹ Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited Feb. 15, 2022).

⁵⁰ See Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 15, 2022).

policies to correct security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.⁵¹

77. The FTC recommends that companies not maintain PI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.⁵²

78. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.⁵³

⁵¹ *Id.*

⁵² *See supra* note 51.

⁵³ *See* Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, available at: <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited Feb. 15, 2022).

79. Failing to take basic security measures in designing and implementing their computer systems and securing Plaintiffs' and Class Members' PI, Defendants allowed thieves to access and collect individuals' PI. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiffs' and Class Members' PI. Defendants' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

80. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that failure to restrict access to information⁵⁴ and failure to segregate access to information⁵⁵ may violate the FTC Act.

81. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, including driver's license numbers and other motor vehicle records (i.e., PI) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

F. Defendants Failed to Comply with Industry Standards

82. Several best practices have been identified that at a minimum should be implemented by companies like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

⁵⁴ *In the Matter of LabMD, Inc.*, Dkt. No. 9357, Slip Opinion, at 15 ("Procedures should be in place that restrict users' access to only that information for which they have a legitimate need."), available at: <https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf>.

⁵⁵ *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (companies should use "readily available security measures to limit access between" data storage systems).

malware software; encryption, making data unreadable without a key; multi-factor authentication; backing up data; and limiting which employees can access sensitive data.

83. Other best cybersecurity practices that are standard in the Defendants' industry, and one or more of which, upon information and belief, Defendants did not employ, include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protecting against any possible communication system; and training staff regarding critical points.

84. Upon information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

85. These foregoing frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Unauthorized Data Disclosure.

G. Defendants' Actions Contravene the Purpose of the Driver's Privacy Protection Act

86. Prior to the enactment of the Driver's Privacy Protection Act, Congress found that most states freely turned over DMV information to whomever requested it with only few restrictions. 137 Cong. Rec. 27,327 (1993).

87. Due to this lack of restrictions, Congress grew concerned that potential criminals could easily access home addresses and telephone numbers of potential victims. 140 Cong. Rec. 7929 (1994) (statement of Rep. Porter Goss).

88. These concerns did, in fact, materialize in the occurrence of crime, harassment, and stalking. Most notably, in 1989, a stalker shot and killed Rebecca Schaeffer, an upcoming actress, after obtaining her unlisted home address from the California DMV. 137 Cong. Rec. 27,327 (1993). In advocating for the DPPA, Representative Jim Moran (D-VA) recounted thieves using information from the DMV to learn home addresses and commit burglary and theft. 137 Cong. Rec. 27,327 (1993). Similarly, Senator Barbara Boxer (D-CA) explained how a man used the DMV to obtain the home addresses of several young women and sent them harassing letters. 39 Cong. Rec. 29,466 (1993). In another instance, a woman who visited a clinic that performed abortions found black balloons outside her home after a group of anti-abortion activists sought to harass her upon seeing her car in the clinic's parking lot. 139 Cong. Rec. 29,462 (1993) (statement of Sen. Chuck Robb).

89. In light of public outrage over the Schaeffer murder and growing concern for the threat to public safety that free access to DMV records posed, Congress enacted the

DPPA “to protect the personal privacy and safety of licensed drivers consistent with the legitimate needs of business and government.” S. Res. 1589, 103rd Cong. §1(b), 139 Cong. Rec. 26,266 (1993) (enacted).

90. Additionally, in enacting the DPPA, Congress was motivated by its “[c]oncern[] that personal information collected by States in the licensing of motor vehicle drivers was being released – even sold – with resulting loss of privacy for many persons.” *Akkawi v. Sadr*, 2:20-CV-01034-MCE-AC, 2021 WL 3912151, at *4 (E.D. Cal. Sept. 1, 2021) (citing *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (alterations in original)). The sale of private information like driver’s license numbers and other motor vehicle records was the exact impetus for the DPPA’s passage.

91. As such, Congress sought to expressly prohibit “disclosing personal information obtained by the department in connection with a motor vehicle record.” *Chamber of Commerce of United States v. City of Seattle*, 274 F. Supp. 3d 1140, 1154 (W.D. Wash. 2017). Driver’s license numbers are thus explicitly listed as “personal information” from “motor vehicle records” under the DPPA. *See* 18 U.S.C. 2725(1).

92. The DPPA further states that “[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title.” 18 U.S.C. 2722(a). By making the PI of Plaintiffs and the Class publicly available, Defendants knowingly disclosed the PI of Plaintiffs and Class Members and otherwise ran afoul of the purpose of the DPPA, and threatened the privacy and safety of licensed drivers, for whose protection the statute was enacted. Defendants’ actions constituted a concrete injury and particularized harm to

Plaintiffs and members of the Class, that would not have happened but for Defendants' failure to comply with the DPPA. Plaintiffs were harmed by the public disclosure of their private facts in addition to the other harms enumerated herein.

93. The unauthorized disclosures of information have long been seen as injurious. The common law alone will sometimes protect a person's right to prevent the dissemination of private information. Indeed, it has been said that privacy torts have become well-ensconced in the fabric of American law. And with privacy torts, improper dissemination of information can itself constitute a cognizable injury. Because damages for a violation of an individual's privacy are a quintessential example of damages that are uncertain and possibly unmeasurable, causes of action such as the DPPA provide privacy tort victims with a monetary award calculated without the need of proving actual damages. The DPPA states that "[a] [s]tate department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section." 18 U.S.C. § 2721(a)(1).

94. Defendants had an obligation to use reasonable security measures under the DPPA, which further states that "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." 18 U.S.C. § 2722(a).

95. Thus, the DPPA provides citizens with a private right of action in the event that their private information is knowingly obtained, disclosed, or used in a manner other

than for the enumerated permissible purposes. The DPPA states: “[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter [18 U.S.C. §§ 2721, *et seq.*] shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court.” 18 U.S.C. § 2724(a).

96. The default rule under the DPPA is non-disclosure. The DPPA is structured such that 18 U.S.C. § 2721(a)(1) and 18 U.S.C. § 2722(a) provide the general prohibition on the release and use of motor vehicle information, and § 2721(b) enumerates fourteen specific exceptions to the general prohibition. Disclosing information to cyber criminals is not one of them. Because the PI was disclosed to unauthorized individuals—*i.e.*, cyber criminals—there is no argument to be made that disclosure was “for a permissible purpose.”

97. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

98. [REDACTED]

[REDACTED]

[REDACTED]

99. As a result of Defendants’ failure to prevent the Unauthorized Data Disclosure, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal

with the future consequences of the Unauthorized Data Disclosure; theft of their valuable PI; the actual, imminent, and certainly impeding injury flowing from fraud and identity theft posed by their PI being disclosed to unauthorized recipients and cyber criminals; damages to and diminution in value of their PI; and continued risk to Plaintiffs' and the Class Members' PI, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PI entrusted and used them.

H. Defendants' Breach of Their Duties

100. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. failing to maintain an adequate data security system to reduce the risk of data breaches;
- b. failing to adequately protect consumers' PI;
- c. failing to encrypt consumers' PI;
- d. failing to properly monitor their own data security systems for existing intrusions;
- e. failing to train their employees in the proper handling of data breaches, the protection of PI, and the maintenance of adequate email security practices;
- f. failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

g. failing to adhere to industry standards for cybersecurity.

101. Defendants' inattention to the reality that anyone, especially thieves with various pieces of individuals' PI, could obtain any individual's PI through compromise of Defendants' computer systems left Plaintiffs and Class Members with no ability to protect their sensitive and private information.

102. Defendants had the resources necessary to prevent the Unauthorized Data Disclosure, but neglected to adequately implement data security measures, despite their obligations to protect Plaintiffs' and Class Members' PI from unauthorized disclosure.

103. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the unauthorized access, disclosure, and ultimately, the theft of Plaintiffs' and Class Members' PI.

104. Accordingly, as outlined below, Plaintiffs and Class Members now face a present, ongoing, and increased risk of fraud and identity theft.

I. Harm to Plaintiffs and Class Members

105. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have been placed at an ongoing, imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Unauthorized Data Disclosure on their lives.

106. As previously discussed, PI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years. And, at all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PI of Plaintiffs and Class Members, including information obtained from motor vehicle records, and of the foreseeable consequences that would occur if Defendants’ data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

107. Cornerstone admitted there was unauthorized access to and disclosure of Plaintiffs’ and Class Members’ PI in the Notice Letter, as well as that Plaintiffs’ and Class Members’ PI was likely viewed and accessed from, and taken off of, Cornerstone’s computer networks.⁵⁶ In the letter, Cornerstone also recognized that the unauthorized access and disclosure created imminent harm to Plaintiffs and Class Members—and specifically directed Plaintiffs and Class Members to remain “vigilant and monitor your accounts for suspicious or unusual activity.”⁵⁷

108. The ramifications of Defendants’ disclosure and failure to keep individuals’ PI secure are long lasting and severe. Once PI is disseminated to unauthorized parties, fraudulent use of that information and damage to victims may continue for years.⁵⁸

⁵⁶ See *supra* note 14.

⁵⁷ *Id.*

⁵⁸ 2014 LexisNexis True Cost of Fraud Study, (August 2014), available at: <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last visited Feb. 15, 2022).

109. Plaintiffs' and Class Members' PI is private, valuable, and sensitive in nature as it can be used to commit a lot of different harms and fraud in the hands of the wrong people. Defendants failed to obtain Plaintiffs' and Class Members' consent to disclose such PI to any other person, as required by applicable law and industry standards.

110. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."⁵⁹

111. As a result of Defendants' failure to prevent the Unauthorized Data Disclosure, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

- a. the compromise, publication, theft, and/or unauthorized use of their PI;
- b. out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- c. lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- d. compromise of their credit scores, access to credit, and other financial scores as a result of identity theft and compromised financial and driver's license information;

⁵⁹ U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, available at: <https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Feb. 15, 2022).

- e. inability to access government services such as tax refunds or unemployment benefits because compromise of those accounts not only causes fraud but also makes it impossible to make legitimate claims;
- f. the continued risk to their PI, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PI in its possession; and
- g. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Unauthorized Data Disclosure for the remainder of Plaintiffs' and Class Members' lives.

112. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further misappropriation and theft.

113. To date, other than providing limited credit monitoring and identity protection services, none of which is targeted to driver's license information or designed to combat unemployment benefits fraud, Defendants do not appear to be taking any measures to assist Plaintiffs and Class Members other than simply telling them to be vigilant themselves.

114. Defendants' failure to adequately protect Plaintiffs' and Class Members' PI has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Instead, as Cornerstone's Notice indicates, Defendants are putting the

burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

115. While some harm has begun already, the worst may be yet to come. There may be a time lag between when additional harm occurs versus when it is discovered, and also between when PI is acquired and when it is used.

J. Harm to Plaintiffs

Plaintiff Johnson

116. Plaintiff Johnson received the Notice Letter via mail after August 4, 2022, from Cornerstone advising that it improperly exposed his PI to unauthorized third parties. Plaintiff Johnson has never sought an insurance quote or been a customer of Cornerstone, and did not consent in any way to Cornerstone having, disclosing, using, or redisclosing his PI.

117. Upon receiving the Notice Letter from Cornerstone, Plaintiff Johnson spent time researching his options to respond to the theft of his driver's license number. He spent and continues to spend additional time reviewing his credit and financial documents concerning the security of his identity. This is time Plaintiff Johnson otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

118. Additionally, Plaintiff Johnson has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. He deletes any and all unencrypted, non-password protected electronic documents containing his PI and destroys any

documents that contain any of his PI, or that may contain any information that could otherwise be used to compromise his PI.

119. Plaintiff Johnson suffered actual injury from having his PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) identity fraud; (b) loss of his privacy; and (c) imminent and impending further injury arising from the increased risk of fraud and identity theft.

120. As a result of the Unauthorized Data Disclosure, Plaintiff Johnson was a victim of identity theft, and will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Kirk

121. Plaintiff Kirk received the Notice Letter via mail after August 4, 2022, from Cornerstone advising that it improperly exposed his PI to unauthorized third parties. Plaintiff Kirk has never sought an insurance quote or been a customer of Cornerstone, and did not consent in any way to Cornerstone having, disclosing, using, or redisclosing his PI.

122. Following the Unauthorized Data Disclosure in November 2021 but prior to receiving the Notice Letter in August 2022, Plaintiff Kirk was notified on or about January 13, 2022, that an unauthorized individual applied for a loan in his name for approximately \$4,727.00. Plaintiff Kirk immediately placed a freeze on his credit upon learning of the fraudulent loan application. On or about January 13, 2022, Plaintiff Kirk also filed a police report related to the fraudulent activity.

123. On or about July 25, 2022, Plaintiff Kirk received a phone call from Avis Car Rental's loss prevention department inquiring about the whereabouts of a car they claim

that he rented on March 8, 2022. Plaintiff Kirk explained that he had his identity stolen and did not rent a car.

124. Plaintiff Kirk filed a police report with the Kingsport and Nashville police departments regarding the fraudulent car rental in his name. Plaintiff sent copies of both reports to Avis Car Rental.

125. Avis Car Rental informed Plaintiff Kirk that they would conduct an investigation and let him know the results. To date, Plaintiff has not been notified of the investigation result.

126. Since receiving notice of the above, and the Notice Letter from Cornerstone, Plaintiff Kirk has spent time researching his options to respond to the theft of his driver's license, including freezing his credit, removing the fraudulent loan entry from his credit report, and filing three police reports for the two incidents of fraud he experienced.

127. He spent and continues to spend additional time reviewing his credit and financial documents concerning the security of his identity. This is time Plaintiff Kirk otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

128. Additionally, Plaintiff Kirk has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. He deletes any and all unencrypted, non-password protected electronic documents containing his PI and destroys any documents that contain any of his PI, or that may contain any information that could otherwise be used to compromise his PI.

129. Plaintiff Kirk suffered actual injury from having his PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) identity fraud; (b) loss of his privacy; and (c) imminent and impending further injury arising from the increased risk of fraud and identity theft.

130. The identity theft suffered by Plaintiff Kirk is logically and temporally linked to the Unauthorized Data Disclosure in the same way that other data breach cases have found to be “fairly traceable.” His driver’s license number was stolen directly from Cornerstone’s website by an unauthorized third party who accessed the website for the purpose of stealing PI like Plaintiff Kirk’s driver’s license.

131. As a result of the Unauthorized Data Disclosure, Plaintiff Kirk was a victim of identity theft, and will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Toni Reynolds

132. Plaintiff Toni Reynolds greatly values her privacy and PI. Prior to the Unauthorized Data Disclosure, Plaintiff Reynolds took reasonable steps to maintain the confidentiality of her PI.

133. Plaintiff Reynolds received a letter dated August 4, 2022, from Cornerstone concerning the Unauthorized Data Disclosure. The letter stated that on November 29, 2021, unauthorized actors gained access to “certain agent accounts and leveraged this access to run unauthorized searches in these subscription databases.”⁶⁰ According to Cornerstone’s

⁶⁰ *Cornerstone National Insurance Company Data Breach Notice to Consumers*, Office of Vermont Attorney General (Aug. 4, 2022),

letter, the compromised files contained Plaintiff Reynolds' first name, last name, and driver's license number.⁶¹

134. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Reynolds faces, Cornerstone offered her a 12-month subscription to IDX credit monitoring service and identity theft recovery services with a November 4, 2022, deadline to enroll. However, Plaintiff Reynolds has not signed up for the program, as she does not trust that Cornerstone's chosen vendor can protect her information. Moreover, traditional credit monitoring will not protect against the likely identity theft harm that will result from a compromised driver's license.

135. In response to the Unauthorized Data Disclosure, Plaintiff Reynolds purchased identity theft protection services, paying \$23.99 per month.

136. After the Unauthorized Data Disclosure, Plaintiff Reynolds began experiencing an uptick in suspicious text and telephone calls she attributes to this Unauthorized Data Disclosure.

137. Since learning of the Unauthorized Data Disclosure, Plaintiff Reynolds has spent considerable time reviewing her bank, credit, and debit card statements. Moreover, Plaintiff Reynolds spent this time at Cornerstone's direction. Indeed, in the notice letter Plaintiff Reynolds received, Cornerstone directed her to spend time mitigating her losses with IDX, which would "help [her] resolve issues if [her] identity was compromised."⁶²

<https://ago.vermont.gov/blog/2022/08/05/cornerstone-national-insurance-company-data-breach-notice-to-consumers/> (last visited Sep. 9, 2022).

⁶¹ *Id.*

⁶² *Id.*

138. The Unauthorized Data Disclosure caused Plaintiff Reynolds to suffer significant fear, anxiety, and stress, which has been compounded by the fact Defendants have not been forthright with information about the Unauthorized Data Disclosure.

139. Plaintiff Reynolds plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Unauthorized Data Disclosure, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

140. Additionally, Plaintiff Reynolds is very careful about sharing her PI. She has never knowingly transmitted unencrypted PI over the internet or any other unsecured source.

141. Plaintiff Reynolds stores any documents containing her PI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

142. Plaintiff Reynolds has a continuing interest in ensuring her PI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

143. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Nationwide Class (the "Class") as defined as follows:

Nationwide Class: All persons in the United States whose PI was compromised in the Unauthorized Data Disclosure announced by Cornerstone on or near August 4, 2022.

144. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs Johnson and Reynolds seek certification of the following California state subclass (“California Subclass”):

California Subclass: All persons in California whose PI was compromised in the Unauthorized Data Disclosure announced by Cornerstone on or near August 4, 2022.

145. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiff Kirk seeks certification of the following Tennessee state subclass (“Tennessee Subclass”):

Tennessee Subclass: All persons in Tennessee whose PI was compromised in the Unauthorized Data Disclosure announced by Cornerstone on or near August 4, 2022.

146. The Nationwide Class and California and Tennessee Subclasses are collectively referred to herein as the “Class” unless otherwise stated.

147. Excluded from the proposed Class are any officer or director of Defendants; any officer or director of any affiliate, parent, or subsidiary of Defendants; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge’s staff.

148. **Numerosity.** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately 295,867 individuals whose sensitive data was compromised in the Unauthorized Data

Disclosure. Membership in the Class is readily ascertainable from Defendants' own records.

149. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

- a. Whether Defendants engaged in the wrongful conduct alleged herein;
- b. Whether Defendants' inadequate data security measures were a cause of the Unauthorized Data Disclosure;
- c. Whether Defendants' actions were knowing in improperly disclosing driver's license numbers to unauthorized parties and/or entities;
- d. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PI;
- e. Whether Defendants disclosed PI obtained from the records of Defendants or third parties without the permission or consent of Plaintiffs and the Class;
- f. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the data security breach;
- g. Whether Defendants violated the Drivers' Privacy Protection Act, 18 U.S.C. § 2724,
- h. Whether Defendants were negligent;

- i. Whether Plaintiffs and the Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and
- j. Whether Plaintiffs and the Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

150. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

151. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. All Class Members were subject to the Unauthorized Data Disclosure and had their PI accessed by, used and/or disclosed to unauthorized third parties. Defendants' misconduct impacted all Class Members in the same manner.

152. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

153. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the Class Members pale

compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

154. **Injunctive and Declaratory Relief:** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants, through their uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendants continue to maintain their inadequate security practices, retain possession of Plaintiffs' and Class Members' PI, and have not been forced to change their practices or relinquish PI by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

155. Likewise, particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to whether:

- a. Plaintiffs' and Class Members' PI was accessed and/or acquired by an unauthorized party in the Unauthorized Data Disclosure;

- b. Defendants owed a legal duty to Plaintiffs and Class Members;
- c. Defendants failed to take adequate and reasonable steps to safeguard Plaintiffs' and Class Members' PI;
- d. Defendants failed to adequately monitor their data security systems;
- e. Defendants failed to comply with applicable laws, regulations, and/or industry standards relating to data security amounting to negligence;
- f. Defendants' security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;
- g. Defendants knew or should have known that they did not employ adequate and reasonable measures to keep Plaintiffs' and Class Members' PI secure; and
- h. Defendants' failure to adhere to FTC data security obligations, industry standards, and/or measures recommended by data security experts caused the Unauthorized Data Disclosure.

FIRST CAUSE OF ACTION

Violation of the Drivers' Privacy Protection Act ("DPPA"), 18 U.S.C. § 2721, et seq.

(On behalf of Plaintiffs, the Nationwide Class, and the California and Tennessee Subclasses)

156. Plaintiffs incorporate and reallege the above allegations by reference.

157. Plaintiffs bring this claim against Defendants on behalf of themselves, the Nationwide Class, and the California and Tennessee Subclasses.

158. Pursuant to 18 U.S.C. § 2722(a), “[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title.”

159. Pursuant to 18 U.S.C. § 2721(a)(1), “[a] [s]tate department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section.”

160. The DPPA provides that “[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains.” 18 U.S.C. § 2724.

161. “Person” is defined as “an individual, organization or entity.” 18 U.S.C. § 2725(2). Cornerstone is a “person” under the DPPA.

162. Further, the definition of “disclose” is “to make known or public” or “expose to view.”⁶³ Defendants’ voluntary action of exposing Plaintiffs’ and Class Members’ PI constitutes a knowing disclosure. In particular, Defendants intentionally configured and designed Cornerstone’s online agent portal to generate responses to requests for insurance quotes that included PI from motor vehicle records. In doing so, unauthorized actors were able to access and obtain the PI of Plaintiffs and Class Members for nefarious purposes.

⁶³ <https://www.merriam-webster.com/dictionary/disclose> (last visited Aug. 31, 2022).

163. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

164. Under the DPPA, a “‘motor vehicle record’ means any record that pertains to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.” 18 U.S.C. § 2725(1). Drivers’ license numbers are motor vehicle records and personal information under the DPPA. 18 U.S.C. § 2725(3); *see also Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 943 (7th Cir. 2015).

165. Defendants obtain, use, disclose, resell, and redisclose motor vehicle records from its customers. Defendants obtain motor vehicle records as part of their business operations intended to generate online insurance quotes and/or insurance policy processing for profit.

166. Defendants also obtain motor vehicle records directly from state agencies or through resellers who sell such records. Defendants knowingly obtained and/or disclosed Plaintiffs’ and Class Members’ personal information, which came from a motor vehicle record, for a purpose not permitted under the DPPA.

167. Defendants knowingly used motor vehicle records for uses not permitted by the statute, including sales, and marketing, among other impermissible uses. Defendants’ disclosure of Plaintiffs’ and Class Members’ personal information to unauthorized individuals violated 18 U.S.C. §§ 2722(a) and/or 2721(a)(1).

168. Defendants' disclosure of personal information was not a permitted use under 18 U.S.C. § 2721(b).

169. Defendants knowingly and voluntarily configured and designed their insurance quote application portal system to disclose Plaintiffs' and Class Members' PI to anyone with access who requested an insurance quote, all in direct violation of the DPPA.

170. Defendants failed to use reasonable care in protecting Plaintiffs' and Class Members' PI by installing substandard security measures that failed to protect Plaintiffs' and Class Members' PI and voluntarily disclosed it to cyber criminals through the intentional configuration and design of its insurance quote application portal.

171. Alternatively, Defendants had actual and/or constructive notice of the risk to Plaintiffs' and the Class Members' PI because they should have been aware that failing to incorporate basic security measures in the configuration and design of its online insurance quoting and agent platform, such as authentication of the person requesting the quote, would cause the improper disclosure of Plaintiffs' and Class Members' PI.

172. Further, Cornerstone and Guidewire had actual and or/constructive notice of the February 2021 Cyber Fraud Alert and March 2021 Cyber Fraud Alert Follow-Up which informed Cornerstone and Guidewire that cyber criminals were exploiting cybersecurity flaws on automobile insurance websites who give out driver's license information by stealing nonpublic information, including driver's license numbers.

173. [REDACTED]

[REDACTED]

[REDACTED]

174. Merriam-Webster's dictionary defines "disclose" as "to make known or public," "to expose to view," or, alternatively, "to open up." None of these definitions requires an identified intended recipient. Instead, disclosure is the act of exposure. Whether or not Defendants meant for identifiable third parties to access the information is not relevant. All that is required for a knowing disclosure is a voluntary action.

175. Defendants knowingly failed to protect their computer systems and/or linked their respective public websites and business to systems and/or networks storing, maintaining, and/or obtaining Plaintiffs' and Class Members' PI, including the application and agent portal.

176. Pursuant to 18 U.S.C. § 2724(b)(1)-(4), Plaintiffs seek, on behalf of themselves and members of the Class (1) actual damages, not less than statutory liquidated damages in the amount of \$2,500; (2) punitive damages; (3) reasonable attorneys' fees and costs; and (4) preliminary and equitable relief as the Court determines to be appropriate.

SECOND CAUSE OF ACTION

Negligence

(On behalf of Plaintiffs, the Nationwide Class, and the California and Tennessee Subclasses)

177. Plaintiffs incorporate and reallege the above allegations by reference.

178. Plaintiffs bring this claim against Defendants on behalf of themselves, the Nationwide Class, and the California and Tennessee Subclasses.

179. Defendants owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining, and testing their data security systems to ensure Plaintiffs' and Class Members' PI in Defendants' possession, or that could be accessed by Defendants, was adequately secured and protected.

180. Defendants owed a duty of care to Plaintiffs and Members of the Class to provide security, consistent with industry standards, to ensure that their systems and networks adequately protected PI they stored, maintained, used, and/or obtained.

181. Defendants owed a duty of care to Plaintiffs and Members of the Class because Plaintiffs and Class Members were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in having inadequate data security for private PI without the consent or authorization of the person whose PI was being provided.

182. Unbeknownst to Plaintiffs and Class Members, they were entrusting Defendants with their PI when Defendants obtained their PI from motor vehicle records directly from state agencies or through resellers who sell such records, as well as through other channels. Defendants had an obligation to safeguard Plaintiffs' and Class Members' information and were in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Unauthorized Data Disclosure.

183. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

184. By collecting, storing, using, and profiting from this data, Defendants had a duty of care to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PI in Defendants' possession, custody or control from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems and data storage architecture to ensure that Plaintiffs' and Class Members' PI was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of Defendants' security systems and data storage architecture in a timely manner; (c) limiting access to insurance agent sensitive websites and portals, not over-permissioning, maintaining password and firewall security, and otherwise securing Cornerstone's online agent databases, websites, and portals; (d) timely acting upon all warnings and alerts, including public information, regarding Defendants' security vulnerabilities and potential compromise of the compiled data of Plaintiffs and hundreds of thousands of Class Members; and (e) maintaining data security measures consistent with industry standards.

185. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PI. Defendants' misconduct included failing to

implement the systems, policies, and procedures necessary to prevent the Unauthorized Data Disclosure.

186. Cornerstone acknowledged Defendants' conduct created actual harm to Plaintiffs and Class Members because Cornerstone warned of the potential for identity theft as a result of the Unauthorized Data Disclosure, and offered credit monitoring.

187. Defendants knew, or should have known, of the risks inherent in collecting and storing PI and the importance of adequate security. Defendants knew about—or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

188. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard Plaintiffs' and Class Members' PI.

189. Because Defendants knew that a breach of their systems, especially insurance agent portals and other systems with motor vehicle records, would damage millions of individuals whose PI was inexplicably stored or was accessible, including Plaintiffs and Class Members, Defendants had a duty to adequately protect their data systems and the PI contained and/or accessible therein.

190. Defendants also had independent duties under state and federal laws requiring Defendants to reasonably safeguard Plaintiffs' and Class Members' PI.

191. Defendants also had common law duties to prevent foreseeable harm to Plaintiffs and Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not

only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their PI because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendants knew that it was more likely than not Plaintiffs and other Class Members would be harmed by such theft.

192. Defendants had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PI that was collected and stored on Cornerstone's computer networks.

193. Defendants' duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PI. Various FTC publications and data security breach orders further form the basis of Defendants' duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

194. Defendants knew or should have known that their computing systems and Cornerstone's data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PI.

195. Defendants breached the duties they owed to Plaintiffs and Class Members described above and thus were negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PI of Plaintiffs and Class Members; (b) detect the breach while it was ongoing or promptly after it occurred; (c) maintain

security systems consistent with industry standards; and (d) promptly notify Plaintiffs and Class Members.

196. In engaging in the negligent acts and omissions as alleged herein, which permitted thieves to access Defendants' systems that stored and/or had access to Plaintiffs' and Class Members' PI, Defendants violated Section 5 of the FTC Act, which prohibits "unfair...practices in or affecting commerce." This includes failing to have adequate data security measures and failing to protect Plaintiffs' and the Class Members' PI.

197. Plaintiffs and the Class Members are among the class of persons Section 5 of the FTC Act was designed to protect, and the injuries suffered by Plaintiffs and Class Members are the types of injury Section 5 of the FTC Act was intended to prevent.

198. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members PI would not have been compromised.

199. Neither Plaintiffs nor the other Class Members contributed to the Unauthorized Data Disclosure as described in this Complaint.

200. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or theft of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data

Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports, compromises to credit scores, and access to state and tax benefits and refunds; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendants' possession (and/or Defendants have access to) and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PI in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PI.

THIRD CAUSE OF ACTION

Negligence *Per Se*

(On behalf of Plaintiffs, the Nationwide Class, and the California and Tennessee Subclasses)

201. Plaintiffs incorporate and reallege the above allegations by reference.

202. Plaintiffs bring this claim against Defendants on behalf of themselves, the Nationwide Class, and the California and Tennessee Subclasses

203. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair acts or practices by Defendants of failing to use reasonable measures to protect PI. Various FTC publications and orders also form the basis of Defendants' duty.

204. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PI and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PI obtained, stored, and used and the foreseeable consequences of a data breach on Defendants' systems.

205. Defendants' duty to use reasonable security measures also arose under the DPPA, under which Cornerstone was required to protect the privacy, confidentiality, and integrity of driver's license information and only to use driver's license information in a permissible fashion.

206. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) along with the DPPA constitutes negligence *per se*.

207. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the DPPA, were intended to protect. Plaintiffs and Class Members are within the class of persons that the DPPA was intended to protect against because the DPPA was expressly designed to protect a person's personal information contained in motor vehicle records from unauthorized disclosure.

208. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) and the DPPA were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members. The DPPA was similarly enacted as a direct result of failures to protect consumer privacy like those outlined above,

and is intended to guard against the unauthorized disclosure of personal information from motor vehicle records.

209. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PI; illegal sale of the compromised PI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Unauthorized Data Disclosure reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

FOURTH CAUSE OF ACTION

Violation of the California Consumer Privacy Act,

Cal. Civ. Code § 1798.100, *et seq.*

(On behalf of Plaintiffs Johnson and Reynolds, the Nationwide Class, and California Subclass)

210. Plaintiffs incorporate and reallege the above allegations by reference.

211. Plaintiffs Johnson and Reynolds bring this claim against Defendants Cornerstone and Guidewire on behalf of themselves, the Nationwide Class, and the California Subclass.

212. Plaintiffs Johnson and Reynolds and the California Subclass members are “consumer[s]” as that term is defined in Cal. Civ. Code § 1798.140(g).

213. Cornerstone and Guidewire are “businesses” as that term is defined in Cal. Civ. Code. § 1798.140(c). Cornerstone and Guidewire each collect consumers’ (including Plaintiff Johnson’s and Reynolds’ and California Subclass Members’) personal information and determine the purposes and means of the processing of this personal information (e.g., they collect and allow access to PI for the purpose of analyzing the information for insurance quotes, and design the systems that process and store consumers’ PI). Cornerstone and Guidewire individually annually receive for commercial purposes or share for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers.

214. Plaintiff Johnson’s and Reynolds’ and California Subclass Members’ PI is “nonencrypted and nonredacted personal information” as that term is used in Cal. Civ. Code § 1798.150(a)(1). At a minimum, this PI included the individual’s name and unique identification number issued on government documents (e.g., driver’s license number).

215. The Unauthorized Data Disclosure constitutes “an unauthorized access and exfiltration, theft, or disclosure” pursuant to Cal. Civ. Code § 1798.150(a)(1).

216. Under the CCPA, Defendants Cornerstone and Guidewire had a duty to implement and maintain reasonable security procedures and practices appropriate to the

nature of Plaintiff Johnson's and Reynolds' and California Subclass Members' PI to protect said PI.

217. Cornerstone and Guidewire breached the duty they owed to Plaintiffs Johnson and Reynolds and California Subclass Members by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs Johnson's and Reynolds' and California Subclass Members' PI; (b) detect the Unauthorized Data Disclosure while it was ongoing; and (c) maintain security systems consistent with industry standards.

218. Defendants' breach of the duty they owed to Plaintiffs Johnson and Reynolds and California Subclass Members described above was the direct and proximate cause of the Unauthorized Data Disclosure. As a result, Plaintiffs Johnson and Reynolds and California Subclass Members suffered damages, as described above and as will be proven at trial.

219. Plaintiffs Johnson and Reynolds seek injunctive relief in the form of an order enjoining Defendants from continuing the practices that constituted their breach of the duties owed to Plaintiffs Johnson and Reynolds and California Subclass Members as described above, and to implement improved security procedures and measures, specifically:

- a. Ordering Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to

promptly correct any problems or issues detected by such third-party security auditors,

- b. Ordering Defendants engage third-party security auditors and internal personnel to run automated security monitoring,
- c. Ordering Defendants audit, test, and train their security personnel regarding any new or modified procedures,
- d. Ordering Defendants not to make PI available without adequate and reasonable safeguards in its agent portal or website;
- e. Ordering Defendants not to store PI or make PI accessible in any publicly facing website or portal,
- f. Ordering Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services,
- g. Ordering Defendants conduct regular computer system scanning and security checks; and
- h. Ordering Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a breach.

220. Plaintiffs also seek actual damages, and all other forms of relief available under the CCPA.

221. On or about September 14, 2022, Plaintiff Johnson sent via registered mail the 30-day notice letter to Cornerstone as required under Civil Code section 1798.150, subd. (b).

222. On or about September 16, 2022, Plaintiff Reynolds sent via certified mail the 30-day CCPA Notice letter to Defendant Cornerstone. Cornerstone later sent a response thereto which failed to fully address and cure the violations alleged in the letter (which are now alleged herein).

223. Defendant Cornerstone did not actually cure the noticed violations as required. Cornerstone asserted, without evidence or proof, that they “cured” the above failures to implement reasonable security procedures to prevent unauthorized access of Plaintiff Reynolds’ and California Subclass members’ PI through steps taken by Cornerstone in response to the incident, limited to “a global password reset” and by notifying its “software vendor.” These inadequate, post- attack actions that Cornerstone allegedly took did not retroactively cure the unauthorized access, as it provides no assurance that Plaintiff Reynolds’ and California Subclass members’ PI was not viewed by—and/or is not still in the hands of—unauthorized third parties.

224. On or about December 20, 2022, Plaintiff Reynolds sent via certified mail the 30-day CCPA Notice letter to Defendant Guidewire. Guidewire later sent a response thereto which failed to fully address and cure the violations alleged in the letter (which are now alleged herein).

225. Defendant Guidewire did not actually cure the noticed violations as required. Guidewire asserted that it did not fall under the definition of a “business” under the CCPA,

and did not provide, in the alternative, any information or evidence that it cured, or even attempted to cure, the CCPA violations at issue.

226. On or August 21, 2023, Plaintiff Reynolds sent via certified mail the 30-day CCPA Notice letters to Accredited, James, and Reed-Wiliams. Defendants Accredited, James, and Reed-Wiliams did not respond at all to the 30-day CCPA Notice letters.

227. None of the steps Defendants Cornerstone and Guidewire assert in their responses demonstrate an actual cure of their failure to implement reasonable security measures to protect Plaintiff Reynolds' and California Subclass members' PI, as the steps they assert they have taken are not sufficient to protect Plaintiff Reynolds' and California Subclass members' PI into the future.

228. Defendants' responses are wholly insufficient to demonstrate any "actual cure" of their failures to implement reasonable security to protect Plaintiff Reynolds' and California Class members' information.

229. As Defendants have not "actually cured" the violations, Plaintiffs Johnson and Reynolds and the California Subclass seek statutory damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident, or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses, injunctive relief, reasonable attorneys' fees and costs, and statutory damages. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

FIFTH CAUSE OF ACTION

Violation of the California's Unfair Competition Law,

Cal. Bus. & Prof. Code § 17200, et seq.

(On behalf of Plaintiffs Johnson and Reynolds, the Nationwide Class, and California Subclass)

230. Plaintiffs incorporate and reallege the above allegations by reference.

231. Plaintiffs Johnson and Reynolds bring this claim against Defendants on behalf of themselves, the Nationwide Class, and the California Subclass.

232. By reason of the conduct alleged herein, Defendants engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq.*

233. Cornerstone stored, and Defendants disclosed, and/or provided access to Plaintiffs Johnson's and Reynolds' and Class Members' PI through Cornerstone's online agent portal and insurance quote platform and website.

234. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures in compliance with federal regulations that would have kept Plaintiff Johnson's and Reynolds' and Class Members' PI secure, and prevented the unauthorized disclosure, loss, or misuse of that PI.

Unlawful Business Practices.

235. Defendants violated the DPPA, Section 5(a) of the FTC Act, the GLB Act, and California Civil Code § 1798.81.5(b) by failing to implement and maintain reasonable and appropriate security measures or follow industry standards for data security.

236. If Defendants had complied with these legal requirements, Plaintiff Johnson and Reynolds and Class Members would not have suffered the damages related to the Unauthorized Data Disclosure.

237. Plaintiff Johnson and Reynolds and Class Members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In addition, Plaintiff Johnson's and Reynolds' and Class Members' PI was accessed, disclosed, taken, viewed, and now in the possession of those who will use it for their own advantage, and/or is being sold for value—making it clear that Plaintiff Johnson's and Reynolds' and Class Members' PI is of tangible value. Plaintiff Johnson and Reynolds and Class Members have also suffered consequential out-of-pocket losses for procuring credit freezes, credit protection services, identity theft monitoring, and/or other expenses relating to identity theft losses or protective measures.

Unfair Business Practices.

238. Balancing Test. Defendants engaged in unfair business practices under the “balancing test.” The harm caused by Defendants' actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, none of Defendants' actions or inactions can be said to have had any utility at all. Defendants' failures were clearly injurious to Plaintiffs Johnson and Reynolds and Class Members, directly causing the harms alleged in the Complaint.

239. Tethering Test. Defendants also engaged in unfair business practices under the “tethering test.” Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. (*See, e.g.,*

Cal. Civ. Code § 1798.1, “The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.”; Cal. Civ. Code § 1798.81.5(a), “It is the intent of the Legislature to ensure that personal information about California residents is protected.”; Cal. Bus. & Prof. Code § 22578, “It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.”) Therefore, Defendants’ acts and omissions amount to a violation of the law.

240. FTC Test. Defendants engaged in unfair business practices under the “FTC test.” The harm caused by Defendants’ actions and omissions, as described in detail above, are substantial in that they affect Plaintiffs Johnson and Reynolds and hundreds of thousands of Class Members, and caused them to suffer actual harms. Such harms include actual identity theft, a substantial and continuing risk of identity theft, disclosure of Plaintiffs Johnson’s and Reynolds’ and Class Members’ PI to third parties without their consent, diminution in value of their PI, consequential out-of-pocket losses for procuring credit freezes, credit protection services, identity theft monitoring, and/or other expenses relating to identity theft losses or protective measures. This harm continues for two reasons. First, Plaintiffs Johnson’s and Reynolds’ and Class Members’ PI remains in Defendants’ possession, without adequate protection. Second, Plaintiffs Johnson’s and Reynolds’ and Class Members’ PI is now possessed by those who obtained it without Plaintiffs Johnson’s and Reynolds’ and Class Members’ consent. Defendants’ actions and omissions violated Section 5(a) of the Federal Trade Commission Act. (*See* 15 U.S.C. § 45(n), defining “unfair

acts or practices” as those that “cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition”; *see also, e.g., In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016), failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

241. Plaintiffs Johnson and Reynolds and Class Members suffered injury in fact, and lost money or property as the result of Defendants’ unfair business practices. Plaintiffs Johnson’s and Reynolds’ and Class Members’ PI was improperly accessed, disclosed, and taken and is now in the hands of those who will use it for their own advantage, potentially—and likely—selling the PI for value—making it clear that Plaintiffs Johnson’s and Reynolds’ and Class Members’ PI is of tangible value. Plaintiffs Johnson and Reynolds and Class Members have also suffered consequential out-of-pocket losses for procuring credit freezes, credit protection services, identity theft monitoring, and/or other expenses relating to identity theft losses or protective measures.

242. As a result of Defendants’ unlawful and unfair business practices in violation of the UCL, Plaintiffs Johnson and Reynolds and Class Members are entitled to equitable and injunctive relief, including restitution or disgorgement.

SEVENTH CAUSE OF ACTION

Declaratory and Injunctive Relief

(On behalf of Plaintiffs, the Nationwide Class, and the California and Tennessee Subclasses)

243. Plaintiffs incorporate and reallege the above allegations by reference.

244. Plaintiffs bring this claim against Defendants on behalf of themselves, the Nationwide Class, and the California and Tennessee Subclasses.

245. This Cause of Action is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

246. As previously alleged, Plaintiffs and Class Members had a reasonable expectation that companies such as Defendants, who could access their PI through automated systems and collect untold volumes of PI, would provide adequate security for that PI.

247. Defendants owed a duty of care to Plaintiffs and Class Members requiring them to adequately secure PI.

248. Defendants still possesses PI regarding Plaintiffs and Class Members and still uses it for their insurance business.

249. Since the Unauthorized Data Disclosure, Defendants have announced few if any changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Unauthorized Data Disclosure to occur and, thereby, prevent further attacks. The only comments in the notice of data breach were vague, unclear, and noncommittal.

250. The Unauthorized Data Disclosure caused actual harm because of Defendants' failure to fulfill their duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendants' failure to address the security failings that lead to such exposure.

251. There is no reason to believe that Defendants' security measures are more adequate now than they were before the Unauthorized Data Disclosure to meet Defendants' legal duties.

252. An actual controversy has arisen in the wake of the Unauthorized Data Disclosure regarding Defendants' present and prospective common law and other duties to reasonably safeguard their customers' PI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PI. Plaintiffs remain at ongoing and imminent risk that further compromises of their PI will occur in the future.

253. Plaintiffs, therefore, seek a declaration (1) that Defendants' existing security measures do not comply with their duties of care to provide adequate security, and (2) that

to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

- a. Ordering Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,
- b. Ordering Defendants engage third-party security auditors and internal personnel to run automated security monitoring,
- c. Ordering Defendants audit, test, and train their security personnel regarding any new or modified procedures,
- d. Ordering Defendants not to make PI available on any publicly-facing webpage and to adequately secure PI in any website, portal, agent system, or network computer system,
- e. Ordering Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services,
- f. Ordering Defendants to conduct regular computer system scanning and security checks; and
- g. Ordering Defendants to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a breach.

254. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another unauthorized data disclosure by Defendants. The risk of another such disclosure is real, immediate, and substantial. If another disclosure occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

255. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another unauthorized data disclosure occurs because of Defendants, Plaintiffs and Class Members will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have pre-existing legal obligations to employ such measures.

256. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data disclosure by Defendants, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose PI would be further compromised.

EIGHTH CAUSE OF ACTION

Breach of Contract to Which Plaintiffs and the Class are Third-Party Beneficiaries

(On behalf of Plaintiffs, the Nationwide Class, and the California and Tennessee Subclasses)

257. Plaintiffs incorporate and reallege the above allegations by reference.

258. Plaintiffs bring this claim against Defendant Guidewire on behalf of themselves, the Nationwide Class, and the California and Tennessee Subclasses.

259. [REDACTED]

260. [REDACTED]

261. [REDACTED]

262. [REDACTED]

263. [REDACTED]

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully request the Court enter an order:

- a. Certifying the proposed Class as requested herein,
- b. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class Counsel,
- c. Finding that Defendants engaged in the unlawful conduct as alleged herein,
- d. Granting injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;
- e. Awarding Plaintiffs and Class Members damages,
- f. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest on all amounts awarded,
- g. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and
- h. Granting such other relief as the Court deems just and proper.

VI. DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class of all others similarly situated, hereby demand a trial by jury as to all matters so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: September 28, 2023

Respectfully submitted,

/s/ Kate M. Baxter-Kauf

Kate M. Baxter-Kauf (MN #0392037)

kmbaxter-kauf@locklaw.com

Karen Hanson Riebel (MN #0219770)

khriebel@locklaw.com

Mauren Kane Berg (MN # 033344X)

mkberg@locklaw.com

LOCKRIDGE GRINDAL NAUEN P.L.L.P.

100 Washington Avenue South, Suite 2200

Minneapolis, MN 55401

Tel.: (612) 339-6900; Fax: (612) 339-0981

Maureen M. Brady (MO # 57800)

mbrady@mcsbanebradylaw.com

MCSHANE & BRADY, LLC

1656 Washington, Ste. 120

Kansas City, MO 64108

Tel.: (816) 888-8010; Fax: (816) 332-6295

Rachele R. Byrd (*pro hac vice*)

byrd@whafh.com

Alex Tramontano (*pro hac vice*)

tramontano@whafh.com

WOLF HALDENSTEIN ADLER

FREEMAN & HERZ LLP

750 B Street, Suite 1820

San Diego, CA 9211

Tel.: (619) 239-4599; Fax: (619) 234-4599

Interim Co-Lead Class Counsel

Gayle M. Blatt

gmb@cglaw.com

P. Camille Guerra

camille@cglaw.com

CASEY GERRY SCHENK

FRANCAVILLA BLATT & PENFIELD, LLP

110 Laurel Street

San Diego, CA 92101

Tel.: (619) 238-1811; Fax: (619) 544-9232

M. Anderson Berry (*pro hac vice*)

aberry@justice4you.com

Gregory Haroutunian (*pro hac vice*)

gharoutunian@justice4you.com

**CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.**

865 Howe Avenue

Sacramento, CA 95825

Tel.: (916) 239-4778; Fax: (916) 924-1829

Attorneys for Plaintiffs and the putative Class